



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,361	10/21/2003	Jeffrey Bruce Lotspiech	ARC920030093US1	1410
67232	7590	10/17/2007	EXAMINER	
CANTOR COLBURN, LLP - IBM ARC DIVISION 55 GRIFFIN ROAD SOUTH BLOOMFIELD, CT 06002			TRAN, ELLEN C	
ART UNIT		PAPER NUMBER		
2134				
MAIL DATE		DELIVERY MODE		
10/17/2007		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/691,361	LOTSPIECH ET AL.	
Examiner	Art Unit		
Ellen C. Tran	2134		

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
 - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
 - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 6/22/2007, 7/17/2007, & 9/28/2007.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,4,6-8,11,13-16,19-23 and 26-99 is/are pending in the application.
4a) Of the above claim(s) 16, 19-23, and 26-97 is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1,4,6-8,11,13-15,98 and 99 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen A.
ELLEN A.
PATENT TAFT
APT EXAMINER
2134

Attachment(s)

- 1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date

4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. 28 Sept. 2007

5) Notice of Informal Patent Application

6) Other:

Detailed Action

1. This action is responsive to communication filed on: 22 June 2007, 17 July 2007, as well as an Examiner Initiated interview on 28 September 2007. Note no agreement was reached with respect to the Examiner Initiated Interview and suggested amendments to the claims, therefore the below rejection is applied.

2. Claims 1, 4, 6-8, 11, 13-15, 98, and 99, are currently pending in this application.

Claims 1 and 8 are independent claims. Claims 1 and 8 have been amended. Claims 2-3, 5, 9-10, 12, 17, 18, , 24, and 25 have been cancelled. Claims 98 and 99 are new. Amendment to the claims is accepted. Claims 16, 19-23, and 26-97 were previously withdrawn.

Response to Arguments

3. Applicant's arguments filed 3 July 2007 have been fully considered however they are not persuasive where noted below, or moot due to new grounds of rejection.

I) In response to applicant's argument on 22 June beginning on page 19, "*Applicant respectfully traverse this rejection and submit that Xu does not describe the removal of a device from the plurality of devices in a network while protecting a content from unauthorized use or distribution ... Applicants respectfully submit that the foregoing excerpt does not disclose the protection of the content from a authorized use or distribution*".

The rejection below has been updated to account for the amended claim. See IBM Response to DVB-CPT Call for Proposals for Content & Copy Management: xCP Cluster Protocol (hereinafter IBM Oct. 2001) on page 7, paragraphs 4-5.

II) In response to applicant's argument on 22 June on page 20, "*Applicant respectfully submit that Xu does not describe tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table.*

The Examiner disagrees to argument presented. Xu teaches the feature of an apparatus requesting a start time and an end time this is recorded in a database. Note the request is interpreted equivalent to 'tentatively marking' in addition the 'authorization table' is considered equivalent to the database that is managed and charged see Xu col. 3, lines 48-67 as well as Xu col. 7, lines 21-36.

III) In response to applicant's argument on 22 June beginning on page 20, "*More specifically, Xu clarifies that: "IP Multicast is a receiver-based protocol. A receiver subscribes to a multicast session group by sending a join message to the multicast session group. Since the network infrastructure delivers the traffic to each member of the multicast session group, the sender does not need to maintain a list of receivers ... Therefore, contrary to Xu's teaching, the present invention maintains a list of networked devices. As a result, Xu teaches away from the present invention.*

The Examiner disagrees to argument presented. The claims are directed to “securely removing a device from at least one of a plurality of devices in a network”, using a reasonable interpretation the Examiner interprets a multicast group equivalent to ‘a plurality of devices in a network’. Nothing in the claims indicates that the plurality of devices each maintain a list of receivers. Although the claims are interpreted in light of the specification, limitations from the specification are not placed into the claims.

IV) In response to applicant’s argument on 22 June on page 21, “*In addition, Applicants respectfully submit that Xu does not tentatively mark the device to be removed, as clarified in the present amendment to claim 1. Furthermore, Applicant submit that Xu does not disclose that the device marked for removal automatically acknowledges the removal as recited in claim 1.*

The Examiner disagrees to argument presented. As noted above Xu in col. 3, lines 48-67 discloses that devices in a multicast group set start times and end times, in addition Xu teaches that the devices have the option of modifying these start and end times by sending additional request, therefore the Examiner interprets the start and end times recorded equivalent to ‘tentative’. Furthermore it is obvious that the terminal acknowledges the end time or ‘removal’ by not extending or shortening the end time.

V) In response to applicant’s argument on 22 June beginning on page 21, “*Applicants agree with the Examiner that: “the following is not explicitly taught in ‘883: “calculating an encryption key for a protected content in the network, based at least in part on a list of the plurality of devices in the network” ... The Examiner resorts to Alve as describing: “An*

exemplary method includes receiving content at a user's device. The received content is encrypted with a content key ... Alve does not describe the present invention as a whole, in that Alve does not teach the elements of claim 1".

This argument is moot due to the amended rejection.

VI) In response to applicant's argument on 22 June beginning on page 22, "*As a result, the hypothetical combination of Xu and Alve will not consider the present invention as a whole, necessitating the finding of non-compliance with the following legal standard/authority, which is cited herein in support of the finding on non-obviousness ... Applicants respectfully submit that the Examiner provided a general reason for the desirability of the combination of Xu and Alve, in hindsight. More specifically, the foregoing reason provided by the Examiner is generic and insufficiently specific".*

This argument is moot due to the amended rejection.

VII) In response to applicant's argument on 17 July on page 16, "*Claim 1 recites, inter alia, "calculating an encryption key for a protected content in network, based at least in part on a list of the plurality of devices in the network ... recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table." Xu fail to teach this feature ... Recognizing this deficiency, the Examiner cites to Alve as allegedly teaching calculating a key based on a list of devices. Alve, however, fail to teach this feature. Alve does teach a domain key, but does not teach calculating this key,*

or recalculating, based on a list of devices ... Thus, even if Xu and Alve are combined, the features of claim 1 do not result".

This argument is moot due to the amended rejection.

VIII) In response to applicant's argument on 17 July beginning on page 16, "*Claim 8 recites features similar to those discussed above with reference to claim 1 and is patentable over Xu in view of Alve for at least the reason advanced with reference to claim 1*".

This argument is moot due to the amended rejection.

IX) In response to applicant's argument on 17 July on page 17, "*Further, new claims 98 and 99 recite how the encryption key is computed. These features are completely lacking in Xu and Alve. In view of the foregoing remarks and amendment, Applicants submit that the above-identified application is now in condition for allowance*".

This argument is moot due to the amended rejection.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 1, 4, 6-8, 11, 13-15**, are rejected under 35 U.S.C. 103(a) as being unpatentable over IBM Response to DVB-CPT Call for Proposals for Content & Copy Management: xCP

Cluster Protocol (hereinafter IBM Oct. 2001) in view of Xu et al. US Patent No. 6,965,883 (hereinafter '883).

As to independent claim 1, “A method for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the method comprising: calculating an encryption key for a protected content in the network, based at least in part on a list of the plurality of devices in the network” is taught in IBM Oct. 2001 on page 7, paragraphs 4-5 “Each piece of content or each content stream in the home is protected with a unique key. These keys are called title keys. Each title key is encrypted with the master key for the particular home, called the binding key. To play content, a device reads the encrypted title key embedded in the content file and decrypts it with the binding key. Then, with the title key, the device decrypts the content itself. Thus, the binding key is important secret in a given network. It is calculated as the cryptographic hash of three quantities: the media key, the network’s binding ID, and the network’s authorization table. The media key is in turn, calculated from the media key block. This is the calculation that separates the compliant devices from the circumvention devices, and is the basis of the renewability in the system. If the media key block is up-to-date, no known circumvention device will be able to calculate the correct media key from it.”, note the circumvent devices are interpreted to be equivalent to the removed device, the content is protected by encryption with an up to date key;

“recalculating the encryption key for all devices remaining in the network and the protected content, using the modified list; and the authorization table” is shown in IBM Oct.

2001 page 7, paragraph 9 "The binding key will change whenever: 1. A new device is introduced into the home (changing the authorization table)"

"and reencrypting the protected content with the recalculated encryption key" is disclosed in IBM Oct. 2001 page 7, paragraph 10 "Every time the binding key changes, all devices in the cluster shall re-encrypt all title keys. To do this, a device must first decrypt the title key using the old binding key, and then re-encrypt it using the new binding key".
the following is not explicitly taught in IBM Oct. 2001:

"tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table; however '883 teaches "Group membership management 122 maintains the group membership information for every terminal on the same multicast link and is responsible for determining the join status of each terminal. Multicast security unit 123 is responsible for sending decryption key 118 to user terminal 110. Optionally, multicast security unit 123 may encrypt the multicast data from multicast server 190 before it is sent to user terminal 110. Multicast security unit 123 sends decryption key 118 when the user initially joins a multicast session. Multicast security unit 123 updates decryption key 118 either when another multicast user terminates the session or at discrete time intervals" in col. 7, lines 4-16;

"the device marked for removal automatically acknowledging the removal" however '883 teaches a device sending a message to be removed it is acknowledging its removal in col. 14, lines 12-20,;

"automatically recording the removal of the device in the authorization table" however '883 teaches updating a database of authorized devices in col. 7, lines 4-16;

It would have been obvious to one of ordinary skill in the art at the time of the invention of a DVB compliant copy protection taught in IBM Oct. 2001 to include a means to record when a device is removed from a network. One of ordinary skill in the art would have been motivated to perform such a modification because a means is needed to determine the cost of receiving content protected data see '883 (col. 3, lines 32 et seq.) "Thus, there is a need for a system, method, and computer program product for calculating a cost of receiving multicast data from a multicast session. The system, method, and computer program product will calculate the cost of receiving multicast data based on either the elapsed time that a user connects to a multicast session, or the volume of data received at a destination during the connection period. The system, method, and computer program product disclosed herein establish a secure billing system for multicast services in a network that provides link level multicasting".

As to dependent claim 4, "wherein recalculating the encryption key comprises including a key management block in the calculation" is taught in IBM Oct. 2001 page 7, paragraph 9.

As to dependent claim 6, "wherein recalculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device to be removed" is shown in IBM Oct. 2001 on page 7, paragraph 8.

As to dependent claim 7, "wherein the protected content is encrypted with a title key; and further comprising reencrypting the title key with the recalculated encryption key" is disclosed in IBM Oct. 2001 page 7, paragraph 4.

As dependent claim 98, "calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding

ID associated with each of the devices on the list and a hash" is taught in IBM Oct. 2001 page 7, paragraph 5.

As to independent claim 8, this claim is directed to the system performing the method of claim 1; therefore it is rejected along similar rationale.

As to dependent claims 11, 13, 14, and 99, these claims contain substantially similar subject matter as claims 4, 6, 7, and 98; therefore they are rejected along similar rationale.

As to dependent claim 15, "wherein the plurality of devices comprise any one or more of: a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device" is taught in IBM Oct. 2001 page 6 note the picture shows the plurality of devices.

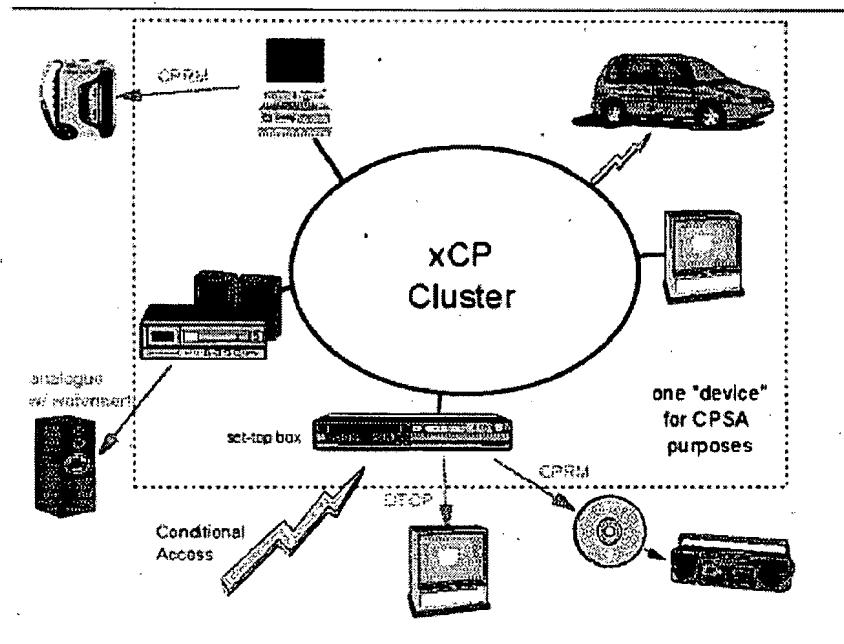


Figure 1 - Relationship of xCP Cluster to the Copy Protection System Architecture

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 7:30 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

Art Unit: 2134

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Ellen Tran
Patent Examiner
Technology Center 2134
13 October 2007